NOTAT

Status på programmet for BPI - Fællesoffentlige styregruppe for infrastruktur i Brugerportalsinitiativet, den 6. december 2016

Dato: 28. november 2016

Sags ID: SAG-2016-06318
Dok. ID: 2276828

E-mail: FRWJ@kl.dk
Direkte: 3370 3301

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

1. Scope

1.1. Sikkerhedsarkitektur

Det indstilles på mødet den 6. december at den fællesoffentlige styregruppe for infrastruktur i Brugerportalsinitiativet godkender PwCs leverancer på baggrund af ledelsesresumeet og indstiller det til godkendelse i styregruppen for IT i folkeskolen den 12. december 2016. Leverancerne omfatter:

- ***Data Protection Impact Assessment – DPIA***: Udgør sammen med Trusselsvurderingen foranalysen som ligger til grund for udarbejdelse af en sikkerhedsarkitekturen.
- ***Trusselsvurdering:*** En identificering og vurdering af trusler.
- ***Sikkerhedsarkitektur:*** Beskrivelse af gavnligt samarbejde ifm. sikkerhed. Sikkerhedsarkitekturen er struktureret omkring både generiske sikkerhedsarkitektoniske overvejelser og konkrete anbefalinger til kommunerne.

1.2. Juridisk afklaring og henvendelse til Datatilsynet

Der er fastsat et møde med Datatilsynet den 11. januar 2017, hvor KL, STIL og KOMBIT deltager. På nuværende tidspunkt er der særligt fokus på sikkerhedsniveauet for Aula på grund af det forestående udbud.

Det er afgørende, at sikkerhedsniveauet for BPI fastsættes korrekt, så der sikres lovmedholdelighed samtidig med at brugervenlighed og sikkerhed balanceres. Udgangspunktet for en fastsættelse af sikkerhedsniveauet for Aula er, at der som udgangspunkt kun i begrænset omfang skal behandles følsomme persondata, da der bl.a. ikke er tale om et sagsbehandlingssystem. Udvalgte områder af systemet skal bl.a. kunne rumme følsomme persondata, hvilket skal håndteres i henhold til Persondataloven og Databeskyttelsesforordningen. I praksis vil håndtering af følsomme persondata kræve to-faktor login iht. Datatilsynets anbefalinger.

./. Fra andre systemer og løsninger har man erfaring med, at et krav om to-faktor login har en væsentlig negativ indflydelse på brugervenligheden, og ydermere på brugernes anvendelse af løsninger. Endvidere findes der pt. ikke et to-faktor login til børn, og det forventes heller ikke at være tilfældet på tidspunktet for idriftsættelse af Aula. En brugervenlig løsning vil derfor på nuværende tidspunkt forventes at skulle isolere behovet for to-faktor login til de områder, der er beregnet til følsomme persondata. Som bilag findes loginmatrix for Aula.

Selvom det kun vil være begrænset omfang, er det på nuværende tidspunkt forventningen at det ift. noget indhold i Aula vil være nødvendigt at anvende to-faktor login. Der vil dog blive lagt vægt på at løsningen i høj grad understøtter særligt medarbejderne i dette, så de belastes mindst muligt.

Dato: 28. november 2016

Sags ID: SAG-2016-06318
Dok. ID: 2276828

E-mail: FRWJ@kl.dk
Direkte: 3370 3301

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Det er blevet besluttet, at dialogen med Datatilsynet baseres på, at der sikres et lovmedholdeligt sikkerhedsniveau iht. den foretagne juridiske afklaring, der samtidig kan leve op til en høj grad af brugervenlighed og vil være muligt for kommunerne at efterleve.

Såfremt Datatilsynet skulle have kommentarer til det sikringsniveau, som præsenteres, kan det efterfølgende vurderes nødvendigt at hæve niveauet. Dette vil i så fald kunne give anledning til et nyt møde med Datatilsynet, men vil ikke have indflydelse på udbuddet af Aula, idet der her er taget højde for, at sikkerhedsniveauet skal kunne justeres.

Juridisk ramme
Persondataloven er den gældende lovgivning frem til 25/5-2018, hvorefter Databeskyttelsesforordningen vil træde i kraft. I BPI klassificeres data iht. den gældende persondatalov og forvaltningslovgivnings fortrolighedsbegreb, men for så vidt muligt at fremtidssikre BPI og Aula ift. det forestående udbud må der også ses mod den kommende Databeskyttelsesforordning. Datatilsynet har givet udtryk for at de vil behandle sagen også i henhold til den kommende Databeskyttelsesforordningen.

Præcisering af den juridiske ramme er udformet på baggrund af en dialog i efteråret 2016 mellem KL, KOMBIT, Ministeriet for Børn, Undervisning og Ligestilling, STIL, Digitaliseringsstyrelsen og Justitsministeriets Databeskyttelseskontor, samt ved vurdering af tidligere afgørelser og praksis på området.
Den foretagne juridiske afklaring medfører følgende rammer for sikkerheden i BPI:

- Eksamenskarakterer (og bemærkninger hertil), testdata og progressionsoplysninger er almindelige persondata - §6, men fortrolige data
- CPR er almindelige persondata - ikke følsomme persondata
- Der kan skelnes mellem følsomme data og tilfældigt opståede følsomme data (eks. i fritekstfelter). Hermed menes områder, der normalt ikke vil indeholde følsomme data, men hvor de i enkelte tilfælde tilfældigt kan opstå, kan håndteres uden to-faktor login, men med eksempelvis tidsklassificering af data eller manuel omklassificering.

Dette betyder, at der er relativt veldefinerede områder, hvor der forefindes følsomme persondata, f.eks. personhenførbare beskeder med følsomt indhold, sikker fildeling og dele af galleri (mediefiler). Hvordan brugergrænsefladen vil håndtere praktisk udførsel af sikkerhed afhænger af leverandøren, ligesom der naturligvis ikke afvises en løsning, der øger sikkerheden. Det er op til leverandøren at finde en løsning der tager hensyn til brugervenligheden.

Mellem parterne er der ved at blive udarbejde et juridisk forudsætningsnotat, der viser ovenstående rammer med henvisning til bl.a. afgørelser. Notatet vil blive vedlagt sagsfremstillingen til Datatilsynet.

1.3. Afslutning af det fællesoffentlige infrastrukturprojekt

I regi af arbejdsgruppen vedr. sikkerhed er det aftalt at med afslutning at det fællesoffentlige infrastrukturprojekt, lukkes handleplanen. Det sker ved at punkterne inddeles i firegrupper:

1. Afsluttede punkter.

Dato: 28. november 2016

Sags ID: SAG-2016-06318
Dok. ID: 2276828

E-mail: FRWJ@kl.dk
Direkte: 3370 3301

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

2. Punkter hvor løsningerne er implementeret, men endnu ikke er tilstrækkeligt formidlet. Disse håndteres på et møde mellem STIL, KL og KOMBIT.
3. Punkter som KL foreslår indgår i det samlede arbejde med governance. Som bilag findes en oversigt til drøftelse.
4. Punkter som det ikke har være muligt at afslutte, og som vil blive håndteret under den kommende driftstyregruppe. Det gælder eks. STILs katalog over yderligere ændringer i UNI-Login, hvor KL den 10. november 2016 har fremsendt kommentarer.

1.4. Forslag til ændring i WS17

Programmet ser en udfordring ift. kommunernes indgåelse af databehandleraftaler med leverandører som anmoder om adgang via snitfladen WS17. Som snitfladen er i dag, kan kommunens administrator tildele adgang til data til leverandører, og altså gøre dem til databehandler ved simpel afkrydsning. Der gøres i snitfladen opmærksom på, at kommunen selv er ansvarlig for at indgå dataaftale med den pågældende leverandør.

Programmet ser i denne sammenhæng en mulighed for at understøtte kommunerne i at indgå databehandleraftaler ved at indbygge dette i selve snitfladen WS17. Programmet foreslår, at der etableres elektronisk databehandleraftale, inddelt i tre dele:

1. Generelle krav til leverandører ifm. databehandling (instrukser). Udarbejdes af KL.
2. Specifikke krav ift. anvendelse af UNI-Login data. Udarbejdes af STIL.
3. Løsnings og/eller kommune specifikke krav. Udarbejdes af kommunen.

For videre afklaring ønskes afholdt en workshop i januar 2017 med kommuner, STIL, leverandører mv. for at afklare behov og muligheder. Forslaget vil være med på den føromtalte emnelog.

2. Tid

2.1. Udbud af Aula

Den 1. december 2016 har KOMBIT sendt udbudsmaterialet på Aula til EU-supply, og det blive tilgængeligt for leverandørerne i løbet af uge 49. Dermed går prækvalifikationsrunden i gang på Aula, hvilket markerer starten på udbuddet.

Leverandørerne har derefter til den 9. januar 2017 til at søge om at blive prækvalificeret. Den 21. januar vil det blive offentliggjort, hvilke fem leverandører der bliver inviteret til at afgive tilbud. Disse tilbud skal være KOMBIT i hænde den 15. maj 2017, og den 30. juni 2017 forventer KOMBIT at underskrive kontrakten med leverandøren af Aula.

Der vil blive lagt en nyhed på KOMBITs website om udbuddets start i begyndelsen af uge 49.

Dato: 28. november 2016

Sags ID: SAG-2016-06318
Dok. ID: 2276828

E-mail: FRWJ@kl.dk
Direkte: 3370 3301

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

3. Økonomi

3.1. Sikkerhedsarkitektur

Den oprindelige tidsplan for analyse og udarbejdelse af sikkerhedsarkitektur- ikke er blevet overholdt. Det har dog ikke influeret på omkostningerne til PwC ift. det oprindelige tilbud. De endelige leverancer fra PwC foreligger den 13. december.

Programmet har dog haft behov for yderligere assistance ift. den juridiske afklaring og den forestående henvendelse til Datatilsynet, og der er blevet lavet en tillægsaftale med PwC på omkring 60 timer. Omkostningerne hertil afholdes af programmet.

4. Kommunikation

4.1. BPI arrangement med fokus på dagtilbud

Den 18. januar 2017 afholder programmet et inspirationsarrangement om BPI og andre digitale aktiviteter i dagtilbud.

På mødet vil bl.a. områdeleder Henrik Boman fra Gladsaxe Kommune fortælle om, hvordan kommunen bruger en digital platform i sine dagtilbud, KOMBIT vil fortælle om arbejdet med den kommende kommunikations- og samarbejdsløsning Aula, som 92 kommuner kommer til at anvende i deres dagtilbud.

4.2. Nyhedsbrev

Der udsendes nyhedsbrev omkring den 10. december, hvor der vil være særligt fokus på udbuddet af Aula, herunder den procedure, KOMBIT anvender til dette udbud, hvor der indgår løbende forhandling og er særligt fokus på at belønne brugervenlighed. KOMBIT forventer også at komme med forslag og inspiration til, hvordan skolerne håndterer datamigreringen fra SkoleIntra til Aula. Derudover fortæller skoleleder Allan Bo Carlsen fra Jægerspris skole i Frederikssund Kommune om, hvordan hans skole implementerer en læringsplatform ved hjælp af kapacitetsteams og egenlæring i fællesskab.

STIL leverer en artikel om, at leverandørerne af læringsplatformene og leverandørerne af de administrative systemer nu er godt i gang med at implementere de nye muligheder i deres systemer, så skolerne kan få glæde af de mange nye tiltag i foråret 2017.

Bilag

Aula Loginmatrix

Udarbejdet af: Thomas Gundel (KOMBIT), med deltagelse af Simon Mark Bøtker-Pedersen (KOMBIT), Jakob Volmer (KOMBIT), Kit Roesen (KL), Gitte Stoltenberg (KL), Lisette Jalking (KL).

Dato: 28. november 2016

Sags ID: SAG-2016-06318
Dok. ID: 2276828

E-mail: FRWJ@kl.dk
Direkte: 3370 3301

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Vedr. login-matricen:

- Der er mange forskellige kombinationsmuligheder for kommunerne, det er "summen" af de faktorer som sættes sammen, der giver sikkerhedsniveauet.
- Alt i matricen understøttes i udbuddet (kravspecifikationen) – valg er et implementeringsspørgsmål
- Der er ikke i udbuddets kravspecifikation skrevet de konkrete løsningsmuligheder (f.eks. B2, B3), det er lagt åbent.

Om to-faktor login muligheder generelt:
A: Forudsætter NemID nøglekort
B: Forudsætter brugernavn-password med brugeroprettelse (UNI-Login eller AD) suppleret med en ekstra faktor
C: Forudsætter personlig mobil device, suppleret med en ekstra faktor

Såfremt implementeringsretningslinjer er overholdt, vil alle login muligheder beskrevet kunne overholde kravene til to-faktor login, med undtagelse af B4, der er en anvendt praksis for internt brug på eget netværk.

Login muligheder:

- A: NemID med nøglekort (enten medarbejdersignatur med nøglekort eller borger NemID med nøglekort)
- B1: Første faktor = login – password på AD e.l. (for børn UNI-Login), anden faktor = enheden selv. *Forudsætter udleveret udstyr, der er personlig for brugeren, så enheden kan tælle som en faktor (f.eks. gennem et device certifikat, der er unikt også for brugeren).*
- B2: Første faktor = login – password på AD e.l. (for børn UNI-Login), anden faktor = sms passcode *(note: kræver mobiltelefon),* google auth. app e.l.
- B3: Første faktor = login – password på AD e.l. (for børn UNI-Login), anden faktor = biometri, f.eks. fingeraftryk *(note: central biometri database, findes ikke for børn)*
- B4: Første faktor = login – password på AD e.l. (for børn UNI-Login), anden faktor = tilstedeværelse på det kommunale net, dvs. at f.eks. PC er på domænet. Er en anvendt praksis for intern brug på eget netværk. Har ikke fuld to-faktor sikkerhed, og kan dermed ikke anvendes over internettet (f.eks. hjemmefra).
- C1: Åben ID Connect "Inspireret af e-Boks modellen, samme brugeroplevelse, men forbedret teknisk".
- C2: Som C1, men for børn "indrullerer/autentificerer" f.eks. en forælder, pædagogisk personale e.l. eleven på enhed, med deres NemID

Bilag

Login matrix:

Dato: 28. november 2016

Sags ID: SAG-2016-06318

Aula 2-faktor login muligheder		PÅ SKOLENS NETVÆRK eller via VPN *				UDENFOR SKOLENS NETVÆRK (f.eks. hjemme)			
Person	Ejerskab af enhed	VIA APP - Personlig mobil enhed	VIA APP - Fælles mobil enhed	VIA BROWSER - Personlig PC	VIA BROWSER - Fælles PC	VIA APP - Personlig mobil enhed	VIA APP - Fælles mobil enhed	VIA BROWSER - Personlig PC	VIA BROWSER - Fælles PC
ANSATTE	Skole/ arbejds-enhed	A, B1, B2, B3, B4, C1	A, B2, B4 (B3. Kan afhænge af biometri løsning)	A, B1, B2, B3, B4	A, B2, B3, B4	A, C1	A	A	A
	Privat ejet enhed	A, B2, B3, C1	A, B2, B3	A, B2, B3	A, B2, B3	A, C1	A	A	A
ELEVER / BØRN (under 15)	Skole/ Arbejds-enhed	B1, B4, C2	B4	B1, B4	B4	C2	Ingen	Ingen	Ingen
	Privat ejet enhed	C2	Ingen	Ingen	Ingen	C2	Ingen	Ingen	Ingen
ELEVER / BØRN (over 15)	Skole/ Arbejds-enhed	A, B1, B4, C1, C2	A, B4	A, B1, B4	A, B4	A, C1, C2	A	A	A
	Privat ejet enhed	A, C1, C2	A	A	A	A, C1, C2	A	A	A
FORÆL-DRE	Skole/ arbejds-enhed	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant
	Privat ejet enhed	Ikke relevant	Ikke relevant	Ikke relevant	Ikke relevant	A, C1	A	A	A

* Model B1, B2 og B3 kan også realiseres ved, at skolen/kommunen udstiller en Identity Provider med to-faktor login, som kan nås via internettet.

Definition af enheder:

- Via **APPs** – mobil enhed: F.eks. tablets, smartphones (primært OIS og Android)
- Via **BROWSER** – PC: F.eks. PC, Chromebooks eller evt. browser på mobil enhed.

Vedr. Bring your own device:
Bring your own device kan håndteres med forskellige grader af kontrol over enheden, hvilket kan håndteres som "skole/arbejdsenhed" hvor skolen har en vis kontrol over enheden, eller som en rent privat ejet enhed.